Quantum Key Distribution Summer School

18 August 2024 - 23 August 2024

SRS

Program

Abstracts

Ueli Maurer: Information-theoretic security

The term information-theoretic cryptography (ITC) refers to cryptographic methods that are secure even against adversaries with unbounded (quantum) computing power, hence not relying on computational hardness assumptions. This lecture first provides a brief overview of cryptography, then presents a constructive way of thinking about cryptographic goals or specifications (e.g. secure communication) and cryptographic methods or protocols (e.g. encryption), then discusses mathematical tools like Shannon's information theory, and finally presents a number of cryptographic methods and protocols relevant for ITC and QKD, including message authentication, one-time-pad encryption, key agreement by public discussion, and privacy amplification.

Norbert Lütkenhaus: Discrete-variable QKD protocols

We will discuss design principles for good QKD protocols and go through some of the basic QKD protocols. Variations of these protocols will illustrate which aspects are essential, and which are protocol choices. We will also discuss methods of practical evaluation of secret key rates for these protocols.

Renato Renner: Foundations of QKD security

Quantum key distribution has the astonishing property that it allows for information-theoretic security, i.e., we can mathematically prove the security of such protocols even against an all-powerful (quantum) adversary. This lecture delves into the foundations of QKD security, first presenting its definition and the underlying motivation. Building on previously introduced concepts such as privacy amplification, we will line out the essential steps involved in a comprehensive security proof. Furthermore, we discuss the central quantities that have to be evaluated in this context and the techniques employed to accomplish this task.

Eleni Diamanti: Implementation of QKD protocols

In this lecture, we will discuss practical aspects of optical systems implementing some important QKD protocols. We will go through typical components of such systems, along with criteria and measures for assessing their performance. We will also present examples of configurations and current challenges related to real-life deployment of QKD in fiber optic and satellite networks, integration aspects, and security against side-channel attacks.

Rotem Arnon-Friedman: Device-independent QKD

In Device-independent QKD (DIQKD) the honest parties, Alice and Bob, do not trust their own devices and, yet, they want to use them to create a shared key. To make such a thing possible, a different type of protocol, based on Bell-inequalities, is required and the security proofs are more demanding. In the lectures, I will explain the basics of DIQKD: The security definition, the fundamental physics that makes DIQKD possible and the main steps of a security proof.

Thomas Jennewein: Space QKD

We will introduce the details and concepts for the space to ground quantum links, and introduce the main technologies required for establishing space QKD including quantum sources, photon detectors, and photon encoding / decoding techniques. We will give an overview on the state of art and mention some of the previous and upcoming quantum space missions, and discuss the big vision outlook for how space-based quantum technologies might achieve global coverage.